# ASA 8.3 und höher: Beispiel für die Konfiguration von FTP- und TFTP-Services aktivieren

## Inhalt



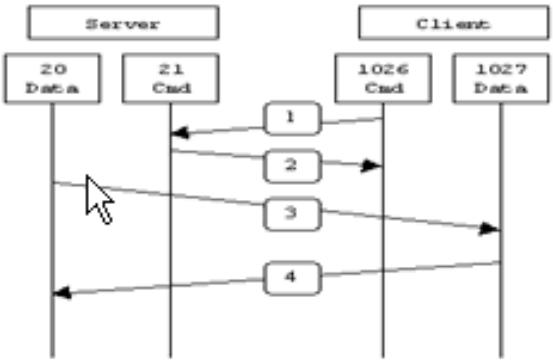
## Einführung

In diesem Dokument werden die Schritte erläutert, die Benutzer außerhalb Ihres Netzwerks für den Zugriff auf FTP- und TFTP-Services in Ihrem DMZ-Netzwerk benötigen.

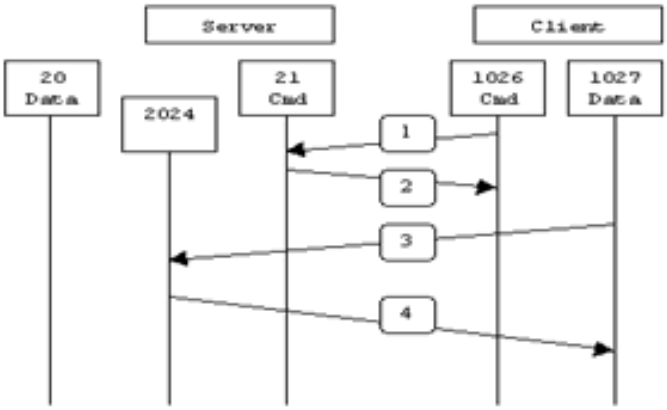
**File Transfer Protocol (FTP)**

Es gibt zwei Arten von FTP:

- Aktiver Modus
- Passiver Modus




Active FTP




Passive FTP

Active FTP :
command : client >1023 -> server 21
data : client >1023 <- server 20

Passive FTP :
command : client >1023 -> server 21
data : client >1023 -> server >1023

Im aktiven FTP-Modus stellt der Client eine Verbindung zwischen einem zufälligen, nicht privilegierten Port (N>1023) und dem Befehlsport (21) des FTP-Servers her. Anschließend überwacht der Client Port N+1 und sendet den FTP-Befehlsanschluss N+1 an den FTP-Server. Der Server stellt dann über seinen lokalen Datenport, Port 20, eine Verbindung zu den angegebenen Datenports des Clients her.

Im passiven FTP-Modus initiiert der Client beide Verbindungen zum Server, wodurch das Problem einer Firewall gelöst wird, die die eingehende Datenport-Verbindung zum Client vom Server filtert. Wenn eine FTP-Verbindung geöffnet wird, öffnet der Client lokal zwei zufällige nicht privilegierte Ports (N>1023 und N+1). Der erste Port kontaktiert den Server an Port 21. Anstatt dann einen **Port-**Befehl auszugeben und dem Server die Verbindung zum Datenport zu ermöglichen, gibt der Client den **PASV-**Befehl aus. Dies führt dazu, dass der Server einen zufälligen nicht privilegierten Port (P>1023) öffnet und den Befehl **port P** zurück an den Client sendet. Der Client initiiert dann die Verbindung von Port N+1 mit Port P am Server, um Daten zu übertragen. Ohne die Konfiguration des **Inspektionsbefehls** auf der Security Appliance funktioniert der FTP-Datenverkehr von internen Benutzern, die in den ausgehenden Datenverkehr geleitet werden, nur im passiven Modus. Außerdem wird Benutzern außerhalb des FTP-Servers der Zugriff verweigert.

Siehe PIX/ASA 7.x: Aktivieren Sie das Konfigurationsbeispiel für FTP/TFTP-Services für die gleiche Konfiguration auf der Cisco Adaptive Security Appliance (ASA) mit Version 8.2 und früher.

### Trivial File Transfer Protocol (TFTP)

TFTP, wie in RFC 1350 beschrieben, ist ein einfaches Protokoll zum Lesen und Schreiben von Dateien zwischen einem TFTP-Server und einem Client. TFTP verwendet UDP-Port 69.

## Voraussetzungen

## Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Es besteht eine grundlegende Kommunikation zwischen den erforderlichen Schnittstellen.
- Sie haben einen konfigurierten FTP-Server im DMZ-Netzwerk konfiguriert.

## Verwendete Komponenten

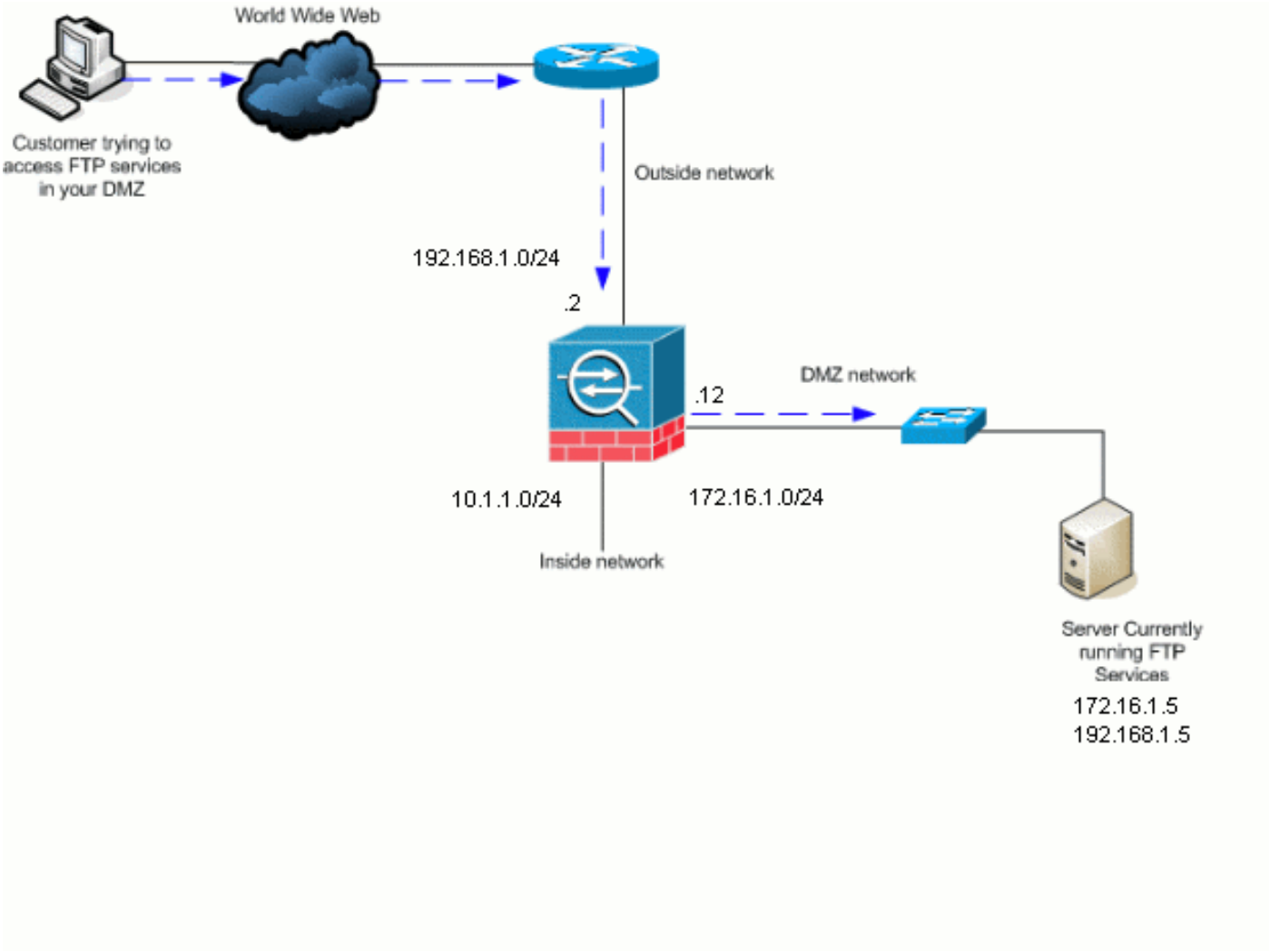
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Adaptive Security Appliance der Serie ASA 5500 mit 8.4(1) Software-Image
- Windows 2003 Server, der FTP-Dienste ausführt
- Windows 2003 Server, der TFTP-Dienste ausführt
- Client-PC außerhalb des Netzwerks

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:




**Hinweis:** Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

## Zugehörige Produkte

Diese Konfiguration kann auch mit Cisco Adaptive Security Appliance 8.3 oder höher verwendet werden.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

# Hintergrundinformationen

Die Security Appliance unterstützt die Anwendungsprüfung über die Adaptive Security Algorithm-Funktion. Mithilfe der Stateful Application Inspection (Stateful-Anwendungsprüfung), die vom Adaptive Security Algorithm verwendet wird, verfolgt die Security Appliance jede Verbindung, die die Firewall passiert, und stellt sicher, dass sie gültig ist. Die Firewall überwacht durch Stateful Inspection auch den Verbindungsstatus, um Informationen zu kompilieren, die in einer Statustabelle gespeichert werden sollen. Bei Verwendung der Statustabelle werden zusätzlich zu vom Administrator definierten Regeln Filterentscheidungen basierend auf dem Kontext festgelegt,

der von Paketen festgelegt wurde, die zuvor über die Firewall weitergeleitet wurden. Die Durchführung von Anwendungsinspektionen umfasst folgende Maßnahmen:

- Identifizieren Sie den Datenverkehr.
- Inspektionen des Datenverkehrs durchführen.
- Aktivieren von Überprüfungen an einer Schnittstelle.

## Erweiterte Protokollverarbeitung

### FTP

Einige Anwendungen erfordern eine besondere Handhabung durch die Cisco Security Appliance-Funktion zur Anwendungsprüfung. Diese Anwendungstypen betten IP-Adressierungsinformationen in das Benutzerdatenpaket ein oder öffnen sekundäre Kanäle an dynamisch zugewiesenen Ports. Die Anwendungsinspektionsfunktion verwendet Network Address Translation (NAT), um den Speicherort integrierter Adressinformationen zu ermitteln.

Neben der Identifizierung eingebetteter Adressinformationen überwacht die Anwendungsinspektionsfunktion Sitzungen, um die Portnummern für sekundäre Kanäle zu ermitteln. Viele Protokolle öffnen sekundäre TCP- oder UDP-Ports, um die Leistung zu verbessern. Die erste Sitzung an einem bekannten Port wird verwendet, um dynamisch zugewiesene Portnummern auszuhandeln. Die Anwendungsinspektionsfunktion überwacht diese Sitzungen, identifiziert die dynamischen Portzuweisungen und ermöglicht den Datenaustausch auf diesen Ports für die Dauer der jeweiligen Sitzungen. Multimedia- und FTP-Anwendungen zeigen dieses Verhalten.

Aufgrund der Verwendung von zwei Ports pro FTP-Sitzung erfordert das FTP-Protokoll eine besondere Handhabung. Wenn das FTP-Protokoll für die Datenübertragung aktiviert ist, werden zwei Ports verwendet: ein Kontrollkanal und ein Datenkanal, der jeweils Port 21 bzw. 20 verwendet. Der Benutzer, der die FTP-Sitzung über den Steuerungskanal initiiert, stellt alle Datenanforderungen über diesen Kanal. Der FTP-Server initiiert dann eine Anforderung, einen Port vom Server-Port 20 zum Computer des Benutzers zu öffnen. FTP verwendet immer Port 20 für die Datenkanalkommunikation. Wenn die FTP-Prüfung auf der Sicherheits-Appliance nicht aktiviert wurde, wird diese Anforderung verworfen, und die FTP-Sitzungen übertragen keine angeforderten Daten. Wenn die FTP-Prüfung auf der Sicherheits-Appliance aktiviert ist, überwacht die Sicherheits-Appliance den Kontrollkanal und versucht, eine Anforderung zum Öffnen des Datenkanals zu erkennen. Das FTP-Protokoll integriert die Datenkanal-Port-Spezifikationen in den Kontrollkanalverkehr, sodass die Security Appliance den Kontrollkanal auf Änderungen an den Datenports überprüfen muss. Wenn die Sicherheits-Appliance eine Anforderung erkennt, erstellt sie vorübergehend eine Öffnung für den Datenkanal-Datenverkehr, der für die Dauer der Sitzung gilt. Auf diese Weise überwacht die FTP-Prüffunktion den Kontrollkanal, identifiziert eine Datenport-Zuweisung und ermöglicht den Datenaustausch auf dem Datenport für die Dauer der Sitzung.

Die Security Appliance prüft standardmäßig Port 21-Verbindungen über die globale Inspection-Klassenzuordnung auf FTP-Datenverkehr. Die Security Appliance erkennt außerdem den Unterschied zwischen einer aktiven und einer passiven FTP-Sitzung. Wenn die FTP-Sitzungen die passive FTP-Datenübertragung unterstützen, erkennt die Security Appliance mit dem Befehl **inspect ftp** die Datenport-Anfrage des Benutzers und öffnet einen neuen Datenport größer als 1023.

Die FTP-Anwendungsinspektion überprüft FTP-Sitzungen und führt vier Aufgaben aus:

- Bereitet eine dynamische sekundäre Datenverbindung vor
- Verfolgt die FTP-Befehlsantwort-Sequenz
- Generiert einen Prüfpfad
- Übersetzt die eingebettete IP-Adresse mithilfe von NAT

Die FTP-Anwendungsinspektion bereitet sekundäre Kanäle für die FTP-Datenübertragung vor. Die Kanäle werden als Reaktion auf einen Datei-Upload, einen Datei-Download oder eine Verzeichnislistenveranstaltung zugewiesen und müssen vorverhandelt werden. Der Port wird über den **PORT** oder **PASV** (227)-Befehl ausgehandelt.

### TFTP

Die TFTP-Prüfung ist standardmäßig aktiviert.

Die Sicherheits-Appliance prüft den TFTP-Datenverkehr und erstellt bei Bedarf dynamisch Verbindungen und Übersetzungen, um die Dateiübertragung zwischen einem TFTP-Client und Server zu ermöglichen. Die Prüfungs-Engine überprüft insbesondere TFTP-Leseanfragen (RRQ), Schreibanfragen (WRQ) und Fehlerbenachrichtigungen (ERROR).

Ein dynamischer sekundärer Kanal und ggf. eine PAT-Übersetzung werden bei Erhalt eines gültigen RRQ oder WRQ zugewiesen. Dieser sekundäre Kanal wird anschließend vom TFTP für die Dateiübertragung oder Fehlerbenachrichtigung verwendet.

Nur der TFTP-Server kann Datenverkehr über den sekundären Kanal initiieren, und es kann maximal ein unvollständiger sekundärer Kanal zwischen dem TFTP-Client und dem Server vorhanden sein. Eine Fehlerbenachrichtigung vom Server schließt den sekundären Kanal.

Die TFTP-Prüfung muss aktiviert werden, wenn TFTP-Datenverkehr mit einer statischen PAT umgeleitet wird.

## Konfigurieren der grundlegenden FTP-Anwendungsüberprüfung

Standardmäßig enthält die Konfiguration eine Richtlinie, die dem gesamten standardmäßigen Anwendungsinspektionsverkehr entspricht und die Überprüfung auf den Datenverkehr an allen Schnittstellen anwendet (eine globale Richtlinie). Der Standarddatenverkehr für die Anwendungsüberprüfung umfasst den Datenverkehr zu den Standardports für jedes Protokoll. Sie können nur eine globale Richtlinie anwenden. Wenn Sie also beispielsweise die globale Richtlinie ändern möchten, um Prüfungen auf nicht standardmäßige Ports anzuwenden oder um standardmäßig nicht aktivierte Überprüfungen hinzuzufügen, müssen Sie die Standardrichtlinie entweder bearbeiten oder deaktivieren und eine neue Richtlinie anwenden. Eine Liste aller Standard-Ports finden Sie in der Standard-Überprüfungsrichtlinie.

1. Geben Sie den **Befehl policy-map global_policy ein**.
   ```
   ASA(config)#policy-map global_policy
   ```

2. Geben Sie den Befehl **class invice_default ein**.
   ```
   ASA(config-pmap)#class inspection_default
   ```

3. Geben Sie den **Befehl inspect FTP (FTP überprüfen)** ein.
   ```
   ASA(config-pmap-c)#inspect FTP
   ```

Es gibt eine Option, den **Befehl inspect FTP strict zu** verwenden. Dieser Befehl erhöht die Sicherheit geschützter Netzwerke, indem verhindert wird, dass ein Webbrowser eingebettete Befehle in FTP-Anfragen sendet.Nachdem Sie die *strenge* Option für eine Schnittstelle aktiviert haben, erzwingt die FTP-Prüfung dieses Verhalten:Ein FTP-Befehl muss bestätigt werden, bevor die Sicherheits-Appliance einen neuen Befehl zulässt.Die Sicherheits-Appliance verwirft eine Verbindung, die eingebettete Befehle sendet.Die Befehle **227** und **PORT** werden überprüft, um sicherzustellen, dass sie nicht in einer Fehlerzeichenfolge angezeigt werden.**Warnung:** Die Verwendung der **Option *strict* kann zum Ausfall von FTP-Clients führen, die nicht streng mit FTP-RFCs kompatibel sind.** Weitere Informationen zur Verwendung der *strict*-Option finden Sie unter Verwenden der strikten Option.

## Beispielkonfiguration

**Gerätename 1**

```
ASA(config)#show running-config

 ASA Version 8.4(1)
!
hostname ASA
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
  no nameif
 no security-level
 no ip address
!
!--- Output is suppressed. !--- Permit inbound FTP
control traffic. access-list 100 extended permit tcp any
host 192.168.1.5 eq ftp
!--- Permit inbound FTP data traffic. access-list 100
extended permit tcp any host 192.168.1.5 eq ftp-data
!
!--- Object groups are created to define the hosts.
object network DMZ
host 172.16.1.5
```

```
object network DMZ-out
host 192.168.1.5
!--- Configure manual NAT nat (DMZ,outside) source
static DMZ DMZ-out
access-group 100 in interface outside
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512

policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
!--- This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA(config)#
```

## Konfigurieren der FTP-Protokollüberprüfung auf einem nicht standardmäßigen TCP-Port

Sie können die FTP Protocol Inspection für nicht standardmäßige TCP-Ports mit folgenden Konfigurationslinien konfigurieren (XXXX durch neue Portnummer ersetzen):

```
access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class
   inspect ftp
```

## Konfigurieren der grundlegenden TFTP-Anwendungsüberprüfung

Standardmäßig enthält die Konfiguration eine Richtlinie, die dem gesamten standardmäßigen Anwendungsinspektionsverkehr entspricht und die Überprüfung auf den Datenverkehr an allen

Schnittstellen anwendet (eine globale Richtlinie). Der Standarddatenverkehr für die Anwendungsüberprüfung umfasst den Datenverkehr zu den Standardports für jedes Protokoll. Sie können nur eine globale Richtlinie anwenden. Wenn Sie die globale Richtlinie beispielsweise ändern möchten, um Prüfungen auf nicht standardmäßige Ports anzuwenden oder um standardmäßig nicht aktivierte Überprüfungen hinzuzufügen, müssen Sie die Standardrichtlinie entweder bearbeiten oder deaktivieren und eine neue Richtlinie anwenden. Eine Liste aller Standard-Ports finden Sie in der Standard-Überprüfungsrichtlinie.

1. Geben Sie den **Befehl policy-map global_policy ein**.
   `ASA(config)#policy-map global_policy`

2. Geben Sie den Befehl **class invice_default ein**.
   `ASA(config-pmap)#class inspection_default`

3. Geben Sie den **Befehl inspect TFTP (TFTP überprüfen)** ein.
   `ASA(config-pmap-c)#inspect TFTP`

## Beispielkonfiguration

**Gerätename 1**

```
ASA(config)#show running-config

 ASA Version 8.4(1)
!
hostname ASA
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
  no nameif
 no security-level
 no ip address
!
!--- Output is suppressed. !--- Permit inbound TFTP
traffic. access-list 100 extended permit udp any host
```

```
192.168.1.5 eq tftp
!
!--- Object groups are created to define the hosts.
object network DMZ
host 172.16.1.5
object network DMZ-out
host 192.168.1.5
!--- Configure manual NAT nat (DMZ,outside) source
static DMZ DMZ-out
access-group 100 in interface outside
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512

policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
!--- This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA(config)#
```

# Überprüfen

Um sicherzustellen, dass die Konfiguration erfolgreich abgeschlossen wurde, verwenden Sie den Befehl **show service-policy**. Beschränken Sie die Ausgabe außerdem auf die FTP-Prüfung nur mit dem **Befehl** show service-policy inspect ftp.

```
ASA#show service-policy inspect ftp
          Global Policy:
           Service-policy: global_policy
            Class-map: inspection_default
             Inspect: ftp, packet 0, drop 0, reste-drop 0
         ASA#
```

# Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung

verfügbar.

## Zugehörige Informationen

- Cisco Adaptive Security Device Manager
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems